No. 17-2

In The Supreme Court of the United States

UNITED STATES OF AMERICA,

Petitioner,

v.

MICROSOFT CORPORATION

On Writ Of Certiorari To The United States Court Of Appeals For The Second Circuit

BRIEF FOR THE STATES OF VERMONT, ALABAMA, ARKANSAS, COLORADO, CONNECTICUT, DELAWARE, FLORIDA, ILLINOIS, INDIANA, IOWA, KANSAS, KENTUCKY, LOUISIANA, MAINE, MARYLAND, MASSACHUSETTS, MICHIGAN, MINNESOTA, MISSISSIPPI, MONTANA, NEBRASKA, NEVADA, NEW JERSEY, NEW MEXICO, NEW YORK, NORTH CAROLINA, OHIO, OKLAHOMA, OREGON, PENNSYLVANIA, RHODE ISLAND, SOUTH CAROLINA, TEXAS, VIRGINIA, WYOMING AND THE COMMONWEALTH OF PUERTO RICO AS *AMICI CURIAE* IN SUPPORT OF PETITIONER

THOMAS J. DONOVAN
Attorney General of the
State of Vermont
BENJAMIN D. BATTLES*
Solicitor General
ELEANOR L.P. SPOTTSWOOD
EVAN P. MEENAN
Assistant Attorneys General
109 State Street
Montpelier, VT 05609
(802) 828-5500
benjamin.battles@vermont.gov

**Counsel of Record*

[Additional Counsel Listed On Signature Page]

COCKLE LEGAL BRIEFS (800) 225-6964
WWW.COCKLELEGALBRIEFS.COM

QUESTION PRESENTED

Whether a United States provider of email services must comply with a probable-cause based warrant issued under 18 U.S.C. § 2703 by making disclosure in the United States of electronic communications within that provider's control, even if the provider has decided to store that material abroad.

TABLE OF CONTENTS

	Page
INTEREST OF AMICI STATES	1
SUMMARY OF ARGUMENT	3
ARGUMENT	5
I. The business decisions of private corporations should not control whether law enforcement can obtain evidence of crimes committed in their jurisdictions	5
II. No extraterritorial conduct occurs when a domestic corporation discloses data the corporation controls, from within the United States, to a domestic law enforcement agency	17
A. Neither *Morrison* nor *RJR Nabisco* supports the Second Circuit's extraterritoriality analysis	17
B. Requiring compliance with the Act's disclosure provisions is consistent with traditional notions of enforcement jurisdiction	19
III. Speculative arguments about international comity and potential legislation do not justify the immediate risks to public safety that will be created if the decision below is affirmed	22
CONCLUSION	25

TABLE OF AUTHORITIES

Page

CASES

Blackmer v. United States, 284 U.S. 421 (1932).....19

Consol. Rendering Co. v. Vermont, 207 U.S. 541 (1908).....20, 21

In re CalECPA, No. CSW 49976 (Cal. Super. Ct., Santa Clara Cty. Oct. 2, 2017) 6, 14

In re Consol. Rendering Co., 66 A. 790 (Vt. 1907) ... 19, 20

In re Info. Associated with One Yahoo Email Address that is Stored at Premises Controlled by Yahoo, No. 17-M-1234, 2017 WL 706307 (E.D. Wis. Feb. 21, 2017).....6, 14

In re Search of Content Stored at Premises Controlled by Google Inc., No. 16-mc-80263, 2017 WL 3478809 (N.D. Cal. Aug. 14, 2017) 14

In re Search of Content Stored at Premises Controlled by Google Inc., No. 16-mc-80263, 2017 WL 1487625 (N.D. Cal. Apr. 25, 2017).....14

In re Search of Info. Associated with Accounts Identified as [redacted]@gmail.com, No. 16-mj-2197, 2017 WL 3263351 (C.D. Cal. July 13, 2017) 14

In re Search of Info. Associated with [redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc., No. 16-mj-757, 2017 WL 3445634 (D.D.C. July 31, 2017)..... 6, 14, 19, 20

TABLE OF AUTHORITIES – Continued

Page

In re Search of Info. Associated with [redacted]@ gmail.com that is Stored at Premises Controlled by Google, Inc., No. 16-mj-757, 2017 WL 2480752 (D.D.C. June 2, 2017) 6, 11, 12, 13, 22

In re Search of Premises Located at [redacted]@ yahoo.com, Stored at Premises Owned, Maintained, Controlled or Operated by Yahoo, Inc., No. 17-mj-1238 (M.D. Fla. Apr. 10, 2017) 14

In re Search Warrant Issued to Google, Inc., No. 5:17-mj-532, 2017 WL 4022806 (N.D. Ala. Sept. 1, 2017) 14

In re Search Warrant Nos. 16-960-M-01 and 16-1061-M to Google, 2017 WL 3535037 (E.D. Pa. Aug. 17, 2017) 14

In re Search Warrant Nos. 16-960-M-01 and 16-1061-M to Google, 232 F. Supp. 3d 708 (E.D. Pa. 2017) 11, 12, 24

In re Search Warrant to Google, Inc., Mag. No. 16-4116, 2017 WL 2985391 (D.N.J. July 10, 2017) 14

In re Search Warrants in Case Nos. 16-MB-00413, 17AG000003, 15AG000082 (Vt. Super. Ct., Addison Cty., July 31, 2017) 11

In re Search Warrant in Case No. 15AG000082 (Google, Inc.), No. 2017-324 (Vt. Oct. 27, 2017) 15

In re Two Email Accounts Stored at Google, Inc., No. 17-M-1235, 2017 WL 2838156 (E.D. Wis. June 30, 2017) 14

TABLE OF AUTHORITIES – Continued

Page

Morrison v. Nat'l Australia Bank Ltd., 561 U.S. 247 (2010) 17

Packingham v. N. Carolina, 137 S. Ct. 1730 (2017) 1

RJR Nabisco, Inc. v. European Cmty., 136 S. Ct. 2090 (2016) 17, 18

CONSTITUTION AND STATUTES

U.S. Const. amend. IV 18

Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508,100 Stat. 1848 (1986) ..... *passim*

18 U.S.C. §§ 2701-2711 1

18 U.S.C. § 2703 ..... *passim*

Vermont Electronic Communications Privacy Act, 13 Vt. Stat. Ann. §§ 8101-8108 ..... 7, 8

Vt. R. Crim. P. 41 8

LEGISLATIVE MATERIALS

132 Cong. Rec. S7993 (daily ed. June 19, 1986) (statement of Sen. Leahy) 24

Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Hearing before the H. Judiciary Comm. (written statement of Richard Littlehale) 15

TABLE OF AUTHORITIES – Continued

Page

Elec. Commc'n Privacy: Hearing on S. 1667 Before the Subcomm. on Patents, Copyrights, and Trademarks of the S. Comm. on the Judiciary, 99th Cong. 39 (1985) (statement of Rep. Kastenmeier) 24

Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights: Hearing before the S. Judiciary Subcomm. on Crime and Terrorism (May 24, 2017) (written statement of Christopher Kelly) 15

OTHER

Correspondence between Chris McDonald and Microsoft Domestic Compliance 16

Google Data Centers: Data and Security, http://www.google.com/about/datacenters/inside/data-security/index.html (last visited Dec. 11, 2017) 11

Google Data Centers: Locations, http://www.google.com/about/datacenters/inside/locations/index.html (last visited July 21, 2017) 12

Justine Jordan, *Email Client Market Share Trends for 2017 (So Far)*, Litmus Software, Inc. (July 17, 2017) 6

Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208 (2004) 7

TABLE OF AUTHORITIES – Continued

Page

Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531 (2005).....18

Letter from Chris McDonald, Special Agent, to Steven Woodson, Director of the Wyoming Div. of Criminal Investigation, re: Microsoft Search Warrant Compliance.....16

Letter from Sara Rodriguez, Google Legal Investigations Support, to Dennis Wygmans, Addison Cty. Deputy State's Attorney (Feb. 6, 2017).....13

Search Warrant, No. 15AG000082 (Vt. Super. Ct., Washington Cty., Dec. 27, 2016).....9

Search Warrant, No. 16-MB-004413 (Vt. Super. Ct., Addison Cty., Jan. 6, 2017).....10

Search Warrant, No. 17AG000003 (Vt. Super. Ct., Chittenden Cty., Jan. 31, 2017).....10

Vt. Internet Crimes Against Children Task Force, www.vt-icac.org (last visited Dec. 10, 2017).....7

INTEREST OF AMICI STATES

This case presents an important legal question that is central to the ability of federal, state, and local law enforcement agencies to investigate and prosecute crime in the digital age.

Amici States investigate and prosecute a wide range of criminal conduct, from drug trafficking and burglary to murder and child sexual exploitation. Email and other electronic communication services provided by companies like Microsoft, Google, Yahoo!, Facebook, and Twitter are ubiquitous in today's world. Indeed, the Court recently described these platforms as "integral to the fabric of our modern society and culture." *Packingham v. N. Carolina*, 137 S. Ct. 1730, 1738 (2017). Not surprisingly, these services are sometimes used to plan and perpetrate crimes. The companies that provide these services control their customers' data and thus often possess evidence that state and local law enforcement agencies need to investigate and prosecute crimes in their jurisdictions.

Under 18 U.S.C. § 2703, a provision of the Stored Communications Act,[1] "a governmental entity," including a state or local law enforcement agency, may require a provider to disclose relevant data "pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State Court, issued using State warrant procedures)

---

[1] 18 U.S.C. §§ 2701-2711. The Stored Communications Act is the common name for Title II of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848.

by a court of competent jurisdiction." 18 U.S.C. § 2703(a). Law enforcement agencies in Amici States, like their federal counterparts, routinely use this "essential investigative tool" in a wide variety of "important criminal investigations around the country." *See* App. 125a (Cabranes, J., dissenting from denial of reh'g en banc) (quotation omitted).

For their own commercial reasons, many providers choose to store data on foreign servers – even when the provider and the customer who generated the data are both in the United States. In some cases, data generated by a single communication may be fragmented and continuously moved from country to country. The content of an email may be stored on a server in one country while the email's attachments are stored on a different server in another country. Indeed, in many instances, the location of data may change between the time when legal process is sought and when it is served.

In this case, on the application of the United States, a federal district court issued a warrant under 18 U.S.C. § 2703 directing respondent Microsoft Corporation to produce the contents of a customer's email account. The court found probable cause to believe the account was being used in furtherance of narcotics trafficking activities in the United States. In the decision below, the court of appeals ordered that the warrant be quashed with respect to data Microsoft had chosen to store on a server in Ireland. According to the panel, it would be an impermissible extraterritorial application of the Stored Communications Act to require

Microsoft to collect and produce data from a foreign server. The court reached this conclusion even though Microsoft could easily access the stored data from its United States offices. As Judge Lynch described in a concurring opinion, this means that Microsoft, or any other provider, "can thwart the government's otherwise justified demand for the emails at issue by the simple expedient of choosing – in its own discretion – to store them on a server in another country." App. 52a.

In recent months, in state and federal courts around the country, providers have relied on the decision below to refuse to comply with search warrants issued under the Stored Communications Act and its state law counterparts. Such refusals have been made even when (i) a court has found probable cause that the email account was used in connection with a domestic crime, (ii) the provider can access the requested data from within the United States, (iii) the account user and the provider are both in the United States, and (iv) law enforcement will receive and review the requested data in the United States. As discussed below, these refusals have had a very real and detrimental impact on Amici States' ability to investigate crimes in their jurisdictions and to protect the safety of their residents.

SUMMARY OF ARGUMENT

The court of appeals' remarkable conclusion that a private company has unfettered discretion to shield evidence of crime from law enforcement – simply by

electronically sending that evidence out of the jurisdiction – is mistaken and should be reversed.

First, the decision below threatens public safety by interfering with the ability of state and local law enforcement agencies to investigate and prosecute serious crimes in their jurisdictions. In courts around the country, Microsoft and other large service providers have relied on the decision to refuse to comply with court-ordered disclosure demands. These refusals are particularly problematic in the context of child sexual exploitation investigations, where the crime itself is often the possession or distribution of digital images of child pornography. If the decision below is affirmed, providers will have carte blanche to place their customers' data beyond the reach of law enforcement by simply storing the data on foreign servers. Fundamental principles of privacy and personal jurisdiction, not the business decisions of private corporations, should dictate whether law enforcement can obtain the evidence it needs to investigate and prosecute these crimes.

Second, nothing in this Court's precedents supports the conclusion reached by the panel below. The Stored Communications Act applies domestically when it requires a domestic corporation to disclose data it controls to a domestic law enforcement agency, in response to legal process from a court of competent jurisdiction. Requiring compliance with the Act's disclosure provisions in this context is also consistent

with traditional notions of enforcement jurisdiction.

Finally, speculative arguments about international comity or potential legislation do not justify the risk to public safety created when state and local prosecutors cannot obtain evidence necessary to investigate and prosecute serious crimes in their jurisdictions.

ARGUMENT

I. The business decisions of private corporations should not control whether law enforcement can obtain evidence of crimes committed in their jurisdictions.

The decision below "affords 'absolute' protection from disclosure to electronic communications stored abroad, regardless of whether they are controlled by a domestic service provider and are accessible from within the United States." App. 126a (Cabranes, J., dissenting from the denial of reh'g en banc) (quoting App. 53a (Lynch, J. concurring)). According to some providers, this is so even when there is no dispute that the communications were generated domestically by a United States resident, a court has determined there is probable cause to believe the communications contain evidence of the commission of a domestic crime, and law enforcement will search the requested data from within the United States.

Although the decision below technically binds only federal courts in the Second Circuit, it is impacting law enforcement agencies nationwide. Several prominent service providers – notably, Microsoft, Google, and Yahoo! – have relied on the decision to resist warrants issued under the Stored Communications Act and its state law counterparts when compliance would require retrieving data from a foreign server.[2] The decision below is therefore directly interfering with Amici States' ability to investigate and prosecute crime in their jurisdictions. The experience of Vermont's Internet Crimes Against Children Task Force is illustrative.

This Vermont task force is part of a network of approximately 61 coordinated task forces representing over 3,500 federal, state, and local law enforcement and prosecutorial agencies. The Vermont Attorney General's Office supervises the task force, whose responsibilities include investigating and prosecuting people who use online communications to sexually

---

[2] *See, e.g., In re Search of Info. Associated with [redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc.*, No. 16-mj-757, 2017 WL 3445634 (D.D.C. July 31, 2017), *aff'g*, 2017 WL 2480752 (D.D.C. June 2, 2017) (Google); *In re Info. Associated with One Yahoo Email Address that is Stored at Premises Controlled by Yahoo*, No. 17-M-1234, 2017 WL 706307 (E.D. Wis. Feb. 21, 2017) (Yahoo); *In re CalECPA*, No. CSW49976 (Cal. Super. Ct., Santa Clara Cty., Oct. 2, 2017) (Microsoft). Together, the services provided by these three companies account for approximately forty percent of all emails opened in the world. Justine Jordan, *Email Client Market Share Trends for 2017 (So Far)*, Litmus Software, Inc. (July 17, 2017), https://litmus.com/blog/email-client-market-share-trends-1h-2017.

exploit children.[3] Since 2008, the task force has prosecuted nearly two hundred cases involving child pornography and child sexual assault or exploitation. In the past two years alone, the task force has obtained hundreds of subpoenas and search warrants, many of which were issued under the federal Stored Communications Act and Vermont's Electronic Communication Privacy Act, 13 Vt. Stat. Ann. §§ 8101-8108.

Under the Stored Communications Act, a government entity may require a provider to disclose a customer's email content by obtaining "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction." 18 U.S.C. § 2703(a). If a court issues the warrant, it is served on the provider like an ordinary subpoena. The provider must then review its files and produce data associated with the relevant user account to the requesting law enforcement agency. The agency then searches the data for evidence of the relevant crime. *See generally* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1219 (2004).

To obtain an SCA warrant, an officer assigned to Vermont's task force first prepares an affidavit demonstrating probable cause that a crime has been committed and that data held by the provider would contain

---

[3] *See* Vt. Internet Crimes Against Children Task Force, www.vt-icac.org (last visited Dec. 10, 2017).

evidence of the commission of that crime. *See generally* Vt. R. Crim. P. 41. A prosecutor then reviews, and if appropriate, approves the warrant application. The officer, and often the prosecutor, then appears before a judge and applies for the warrant. The court may only issue the warrant if it is satisfied, based on substantial evidence, that there is probable cause to believe that the requested data will contain evidence of the commission of a crime. 18 U.S.C. § 2703(a); Vt. R. Crim. P. 41(b), (d).

When a provider relies on an extraterritoriality argument to resist complying with an SCA warrant, it interferes with the task force's ability to investigate and prosecute people who use the provider's products to sexually exploit children. It also limits the task force's ability to identify victims who may still be in danger. And the only justification for these social harms is the provider's business decision to locate some of its servers outside the United States.

The Vermont Attorney General's Office and Addison County State's Attorney's Office, on behalf of the task force, recently litigated three motions to compel in state court against Google. In those actions, Google relied on the decision below to resist warrants issued jointly under the federal Stored Communications Act and Vermont's Electronic Communication Privacy Act, insofar as those warrants required disclosing data stored on foreign servers.[4] The facts of these cases,

---

[4] The Stored Communications Act expressly authorizes government entities to rely on state law and state warrant

described below, demonstrate the serious risks to public safety posed by the court of appeals' decision.

In the first case (the Washington case), the task force obtained warrants to review the contents of two Gmail accounts. The task force sought the warrants after an investigation determined that a Vermont resident, who had a previous criminal conviction for an offense involving sexual misconduct with a child, was in possession of a vast amount of child pornography. At the time the suspect was identified, he was living in a home with two young children. During the investigation, the suspect admitted to the investigating officer that he used his iPhone to exchange images of child pornography, and that he had recently used his phone to send images of his penis to a 12- or 13-year-old girl that he met online. He also admitted to using the two Gmail accounts to exchange images of child pornography. Before the task force could obtain the suspect's phone, he used the factory reset option to delete its contents.[5]

In the second case (the Chittenden case), the task force obtained a warrant to search the contents of one Gmail account. The task force sought the warrant after Google reported to the National Center for Missing and Exploited Children that the account had been used to upload an apparent image of child pornography as

---

procedures when seeking disclosure of electronically stored data. *See* 18 U.S.C. § 2703(a), (b)(1)(A), (b)(1)(B)(i), (c)(1)(A), (c)(2), (d).

[5] Search Warrant, No. 15AG000082 (Vt. Super. Ct., Washington Cty., Dec. 27, 2016) (on file with the Vermont Attorney General's Office).

an attachment to an email. Based on the report, the Center determined the account holder was likely in Vermont at the time of the upload. The Center referred the report to the task force for investigation.[6]

In the third case (the Addison case), the task force obtained warrants to search the contents of five Gmail accounts. The task force sought the warrants after an investigation revealed that the accounts were being used by a Vermont resident as part of an elaborate and long-running scheme to acquire and distribute child pornography and commit sexual assault on multiple young females, including children, in Texas and Vermont.[7]

Thus, each of the three cases shared several important features: (i) the customer whose data was sought lived or was located in Vermont when the crime under investigation was committed; (ii) a court found probable cause to believe a crime occurred in Vermont and that the contents of the customer's email account would contain evidence of that crime; (iii) the court ordered disclosure from Google, a United States company doing business in Vermont and subject to the court's jurisdiction; and (iv) law enforcement would receive and review the responsive data in Vermont. Nonetheless, relying on the decision below, Google resisted

---

[6] Search Warrant, No. 17AG000003 (Vt. Super. Ct., Chittenden Cty., Jan. 31, 2017) (on file with the Vermont Attorney General's Office).

[7] Search Warrant, No. 16-MB-004413 (Vt. Super. Ct., Addison Cty., Jan. 6, 2017) (on file with the Vermont Attorney General's Office).

compliance in each case, and thereby denied investigators access to time-sensitive electronic evidence that could have been used to identify victims and prevent ongoing crime.

As Google explained in the Vermont cases and in similar litigation around the country, only certain of the company's employees in the United States are authorized to respond to legal process. Those employees, however, can access responsive customer data from any computer, anywhere, that is connected to the internet. *E.g.*, *In re Search Warrants in Case Nos. 16-MB-00413, 17AG000003, 15AG000082*, slip op. 2-3 (Vt. Super. Ct., Addison Cty., July 31, 2017);[8] *In re Search of Info.*, 2017 WL 2480752, at *3; *In re Search Warrant Nos. 16-960-M-01 and 16-1061-M to Google*, 232 F. Supp. 3d 708, 712-13 (E.D. Pa. 2017), *aff'd*, 2017 WL 3535037 (E.D. Pa. Aug. 17, 2017).

Because of the structure of its network, however, Google's ability to meaningfully comply with an SCA warrant is severely compromised when it refuses to disclose content that is stored on a foreign server. For its own business reasons, Google divides data from a single customer file into component "chunks" or "shards," which are then automatically copied and moved between a worldwide network of data centers.[9] *In re Search of*

---

[8] *Available at* http://ago.vermont.gov/assets/files/PressReleases/Criminal/Holden%20Google%20Order.pdf (last visited Dec. 8, 2017).

[9] Google Data Centers: Data and Security, http://www.google.com/about/datacenters/inside/data-security/index.html (last visited Dec. 11, 2017). Google's network includes data centers in Belgium,

Info., 2017 WL 2480752, at *3; *In re Search Warrant*, 232 F. Supp. 3d at 712. The location of a customer's data at any given time bears no relationship to the location of the customer who created the data. In a network like Google's, it can be difficult to pinpoint the location of relevant data at all.[10] For example, an email's content, header information, and attachments may be stored on three different servers in three different locations on one day, and on three different servers the next day. *In re Search of Info.*, 2017 WL 2480752, at *3; *In re Search Warrant*, 232 F. Supp. 3d at 712. It is thus possible that the network will change the location of data between the time when legal process is sought and when it is served. *In re Search of Info.*, 2017 WL 2480752, at *3; *In re Search Warrant*, 232 F. Supp. 3d at 712. Moreover, "the shards of data are effectively meaningless on their own – for purposes of an SCA warrant, a recognizable file useful to law enforcement may exist only when its component parts are compiled remotely from within Google's California headquarters and then produced to the government pursuant to a warrant." *In re Search of Info.*, 2017 WL 2480752, at *3.

Before the court of appeals' decision in this case, Google routinely disclosed customer data sought by a

---

Chile, Finland, Ireland, the Netherlands, Singapore, and Taiwan. Google Data Centers: Locations, http://www.google.com/about/datacenters/inside/locations/index.html (last visited Dec. 11, 2017).

[10] Indeed, it is apparently sometimes impossible for Google "to determine the location of the data . . . at any particular point in time." *In re Search Warrant*, 232 F. Supp. 3d at 712.

properly issued SCA warrant, regardless of where the data was stored. *Id.* After the decision below was issued, however, Google reconfigured its search tool to query only domestic servers. *Id.*

In response to the Vermont task force's warrants, Google refused to produce any email content it could not confirm was located in the United States. Particularly problematic in the context of a child pornography investigation was Google's refusal, for several email accounts, "to produce[ ] the attachments to any emails because the attachment files were not confirmed to be stored in the United States." *See, e.g.*, Letter from Sara Rodriguez, Google Legal Investigations Support, to Dennis Wygmans, Addison Cty. Deputy State's Attorney (Feb. 6, 2017) (citing the decision below).[11]

After the State moved to compel Google's disclosures in the three cases, Google voluntarily complied with the warrants in the Addison and Chittenden cases, explaining that it had revised its search protocols and now could locate the requested data on domestic servers. A Vermont trial court granted the State's motion to compel in the Washington case, joining the apparently unanimous chorus of lower courts that

[11] On file with the Vermont Attorney General's Office.

have rejected the panel's analysis in the decision below.[12] *In re Search Warrants*, slip op. 6-9.[13]

Google thereafter agreed to be held in contempt to appeal the order in the Washington case to the Vermont Supreme Court. After this Court granted certiorari in this case, Google stipulated to a dismissal of its state court appeal and finally disclosed the data sought by the task force in the Washington case – *nearly ten months* after a court determined the company had data needed in a serious criminal investigation involving the potentially ongoing sexual exploitation of children by a Vermont resident. *See In re Search Warrant in*

---

[12] *See, e.g.*, *In re Search Warrant Issued to Google, Inc.*, No. 5:17-mj-532, 2017 WL 4022806 (N.D. Ala. Sept. 1, 2017); *In re Search Warrant*, 2017 WL 3535037, *aff'g*, 232 F. Supp. 3d 708; *In re Search of Content Stored at Premises Controlled by Google Inc.*, No. 16-mc-80263, 2017 WL 3478809 (N.D. Cal. Aug. 14, 2017), *aff'g*, 2017 WL 1487625 (N.D. Cal. Apr. 25, 2017); *In re Search of Info*, 2017 WL 3445634, *aff'g*, 2017 WL 2480752; *In re Search of Info. Associated With Accounts Identified as [redacted]@gmail.com*, No. 16-mj-2197, 2017 WL 3263351 (C.D. Cal. July 13, 2017); *In re Search Warrant to Google, Inc.*, Mag. No. 16-4116, 2017 WL 2985391 (D.N.J. July 10, 2017); *In re Two Email Accounts Stored at Google, Inc.*, No. 17-M-1235, 2017 WL 2838156 (E.D. Wis. June 30, 2017); *In re Search of Premises Located at [redacted]@yahoo.com, Stored at Premises Owned, Maintained, Controlled or Operated by Yahoo, Inc.*, No. 17-mj-1238 (M.D. Fla. Apr. 10, 2017); *In re Info. Associated with one Yahoo Email Address*, 2017 WL 706307; *In re CalECPA*, No. CSW49976. Amici States are not aware of any court that has agreed with the Second Circuit's extraterritoriality analysis.

[13] The court ultimately rested its decision on state law grounds. *Id.* at 4-10.

Case No. 15AG000082 (Google, Inc.), No. 2017-324 (Vt. Oct. 27, 2017) (entry order dismissing Google's appeal).

Vermont's experience is not unique. Law enforcement agencies around the country have experienced similar problems because of the decision below.

In Utah, for example, a provider refused to comply with a warrant that sought the contents of an account police knew contained a photograph of the suspect sexually abusing a minor. *See Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights: Hearing before the S. Judiciary Subcomm. on Crime and Terrorism* (May 24, 2017) (written statement of Christopher Kelly 3-4);[14] *Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Hearing before the H. Judiciary Comm.* (written statement of Richard Littlehale 3-4).[15] And in California, a provider recently refused to comply with a warrant for the contents of a cloud account that could be instrumental in determining the timeline and location of a young girl's disappearance and suspected murder. *Id.* Amici States have also learned of providers refusing to comply with SCA warrants for email data in sexual exploitation investigations in a number of other States, including

---

[14] *Available at* https://www.judiciary.senate.gov/meetings/law-enforcement-access-to-data-stored-across-borders-facilitating-cooperation-and-protecting-rights.

[15] *Available at* https://judiciary.house.gov/hearing/data-stored-abroad-ensuring-lawful-access-privacy-protection-digital-era/.

Massachusetts, Indiana, Illinois, Mississippi, New Hampshire, New Jersey, and Texas.

Although these examples involve child exploitation investigations, the problem is far more widespread. Given the ubiquity of email and other electronic communications, this issue can potentially arise in any criminal investigation.

For example, in Sundance, Wyoming, the Bear Lodge motel recently received an arson threat via an email from a Hotmail account, shortly after another local motel had been destroyed by a fire. Law enforcement obtained a warrant to search the contents of the email account and served it on respondent Microsoft approximately one month after the threatening email was sent. According to local law enforcement involved with the case, Microsoft did not respond to the warrant for approximately four months, and then indicated it could not comply and that the warrant was "invalid" because it sought data stored in Ireland. Several weeks later, without explanation, Microsoft complied with the warrant.[16]

---

[16] Letter from Chris McDonald, Special Agent, to Steven Woodson, Director of the Wyoming Div. of Criminal Investigation, re: Microsoft Search Warrant Compliance, *available at* http://www.ago.vermont.gov/assets/files/Signed%20Microsoft%20McDonald%20Letter.pdf (last visited Dec. 12, 2017); Correspondence between Chris McDonald and Microsoft Domestic Compliance, *available at* http://www.ago.vermont.gov/assets/files/Microsoft%20McDonald%20Emails.pdf (last visited Dec. 12, 2017). The description above is based on these documents and conversations with the Wyoming Attorney General's Office. Microsoft disputes this description.

These are just the problems under various providers' current systems. Nothing prevents Microsoft or any other provider from choosing at any time to store all of its customers' data on foreign servers. Under the court of appeals' reasoning, providers have carte blanche to fashion their network architecture so that their customers' data is stored beyond the reach of domestic law enforcement. While that may suit the providers' commercial interests, it poses a serious threat to public safety. Amici States' ability to investigate and prosecute crime in their jurisdictions should not be held hostage by the business decisions of private corporations.

II. No extraterritorial conduct occurs when a domestic corporation discloses data the corporation controls, from within the United States, to a domestic law enforcement agency.

A. Neither *Morrison* nor *RJR Nabisco* supports the Second Circuit's extraterritoriality analysis.

As explained in the United States' brief, the court of appeals erred in concluding that the Stored Communications Act applies extraterritorially when it compels a provider like Microsoft to produce data the provider has chosen to store on a foreign server. U.S. Br. 18-32. That conclusion is contrary to this Court's decisions in *Morrison v. National Australia Bank Ltd.*, 561 U.S. 247 (2010), and *RJR Nabisco, Inc. v. European Community*, 136 S. Ct. 2090 (2016). *Id.* The proper "focus" of Section 2703 is the provider's disclosure of

electronic communications to law enforcement, which occurs entirely within the United States. U.S. Br. 22-26; *see also RJR Nabisco*, 136 S. Ct. at 2101 ("If the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad. . . .").

The result would be no different if the relevant statutory focus was user privacy. U.S. Br. 26-32. No extraterritorial invasion of privacy occurs when a provider's employee uses a computer in this country to retrieve data from a foreign server, and then discloses that data to a domestic law enforcement agency. Indeed, no invasion of privacy occurs at all until the data is disclosed to law enforcement. A provider like Microsoft does not need authorization to move its customer's data from a server in one country to a server in another country. "[I]t already has custody and control of the targeted communications and the legal ability to move them at will." *Id.* at 27. Accordingly, any potential "search" or "seizure," and any consequent invasion of privacy, occurs in the United States. *Id.* at 30-32; *see also* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 551 (2005) (arguing that, for purposes of the Fourth Amendment, "a search occurs when information from or about the data is exposed to possible human observation, such as when it appears on a screen, rather than when it is copied by the hard drive or processed by the computer").[17]

---

[17] Locating a customer's privacy interest abroad makes even less sense when the customer lives in this country and is being investigated for committing a crime in this country. This is

B. Requiring compliance with the Act's disclosure provisions is consistent with traditional notions of enforcement jurisdiction.

Although the technology at issue in this case is new, the underlying legal principle at stake is not. A company should not be permitted to shield evidence of criminal conduct from law enforcement simply by relocating that evidence to a facility the company controls in another jurisdiction.

As one district court recently noted in rejecting the reasoning of the panel below, it is a "well-established principle that courts have the power to exercise authority on people and entities over whom they have personal jurisdiction, including compelling those individuals or entities to retrieve documents from abroad." *In re Search of Info.*, 2017 WL 3445634, at *14; *see also Blackmer v. United States*, 284 U.S. 421, 438 (1932) ("The jurisdiction of the United States over its absent citizen, so far as the binding effect of legislation is concerned, is a jurisdiction in personam, as he is personally bound to take notice of the laws that are applicable to him and obey them.").

The Court made this basic principle clear more than a hundred years ago. In 1906, the Consolidated Rendering Company was headquartered in Boston, Massachusetts, but operated a meat and rendering plant in Burlington, Vermont. *See In re Consol. Rendering Co.*, 66 A. 790, 792 (Vt. 1907), *aff'd*, 207 U.S. 541

---

typically the situation when state and local prosecutors seek SCA warrants. *See above* Section I.

(1908). The State of Vermont, through a grand jury, was investigating four members of the State's board of cattle commissioners for selling diseased meat. *Id.* The grand jury served Consolidated Rendering with a subpoena to produce records regarding the company's dealings with the cattlemen. *Id.* But before the subpoena issued, the company directed its Burlington bookkeeper to send all the company's relevant records to the Boston office. *Id.* at 795.

Despite this, the Vermont courts found the company in contempt for failing to produce the records in Vermont in response to the subpoena. As the Vermont Supreme Court explained, "[t]aking the books [to another jurisdiction] was merely shifting them from one hand to the other." *Id.* at 799. Control was "the essential thing, and not the precise locality where they happened to be when called for." *Id.* No one subject to a court's jurisdiction can evade their "testimonial duty" by sending to another jurisdiction documents "which are required as evidence in legal proceedings here, and refuse to produce them when required by authority of law." *Id.*

This Court affirmed, holding "that a corporation doing business in the state, and protected by its power, may be compelled to produce, before a tribunal of the state, material evidence in the shape of books or papers kept by it in the state, and which are in its custody and control, although, for the moment, outside the borders of the state." *Consol. Rendering Co. v. Vermont*, 207 U.S. 541, 552 (1908). Requiring the company to comply with the subpoena "in no sense" dictated "how the company shall perform its duties and obligations in other

states," rather, it directed "the company doing business in the state and present therein, by its officers or some of them, to do something which it is entirely competent to do, the purpose of which is to enable the tribunal making the investigation under a state statute to perform its duty." *Id.*

This basic principle of jurisdiction is not defeated simply because the Stored Communication Act labels the disclosure mechanism at issue in this case a "warrant" rather than a "subpoena." A warrant issued under the Act is properly understood as "a distinct procedural mechanism from a traditional Rule 41 'search warrant.'" *In re Search of Info.*, 2017 WL 3445634, at *19. It contains the procedural protections of a traditional warrant – notably, the requirement of a judicial finding of probable cause – but once issued, functions much like a subpoena. 18 U.S.C. § 2703(a), (b)(1)(A); U.S. Br. 32-41; *see also* App. 58a-59a (Lynch, J., concurring).

But even if an SCA warrant is viewed as a traditional search warrant, with the consequent territorial limitations, the courts still possess sufficient authority to require a domestic provider to retrieve and disclose data the provider has stored on a foreign server. This is because the provider is subject to the court's jurisdiction and has the data literally in hand, from within the country, at the push of a button. App. 121a ("Extraterritoriality need not be fussed over when the information sought is already within the grasp of a domestic entity served with a warrant.") (Jacobs, J., dissenting from denial of reh'g).

III. Speculative arguments about international comity and potential legislation do not justify the immediate risks to public safety that will be created if the decision below is affirmed.

As discussed above, the rule of law created by the court of appeals threatens public safety by preventing state and local law enforcement from obtaining crucial evidence needed to investigate and prosecute crime and identify victims. *See* Section I. All too often these victims are young children who have been sexually exploited by people using the products of Microsoft and other providers. *Id.* Microsoft, however, has argued that a reversal would threaten international comity and undermine legislative efforts to revise the Stored Communications Act. Those arguments are misplaced. The harms Microsoft cites are speculative, and pale in comparison to the real and immediate consequences of the decision below.

First, concerns of international comity do not justify affirming the decision below. To the contrary, enforcing § 2703 is entirely consistent with this country's international obligations. *See* U.S. Br. 46-52.

Moreover, federal, state, and local law enforcement agencies all routinely obtained SCA warrants before this case was decided by the court of appeals. And providers routinely complied with those warrants. *See, e.g.*, *In re Search of Info.*, 2017 WL 2480752, at *3. As discussed above, the Vermont Internet Crimes Against Children Task Force has obtained hundreds of

subpoenas and warrants under the Stored Communications Act and its state law counterpart, all without international incident. The experience of the other Amici States is comparable.

The nature of these cases makes them extremely unlikely to spark international discord. The task force uses SCA warrants primarily to obtain crucial evidence in child pornography and exploitation cases. The data sought typically includes the pornographic material itself, or key admissions by the suspect. State and local law enforcement around the country also routinely use SCA warrants to investigate a wide variety of other offenses committed in their jurisdictions – *i.e.*, local crimes, most often committed by individuals physically present in the State or municipality. The country where a customer's data is stored may have no connection to the investigation or the crime, and no connection to the customer. The data is stored in the country only because the provider decided that it should be so. The countries are interchangeable and, for some providers, frequently interchanged.

In the unlikely scenario that an SCA warrant does provoke a conflict with foreign law, however, courts in the United States are well-equipped to address any potential problems through well-established conflict of laws principles. *See* U.S. Br. 50-52. "And more to the point, the possibility of a future conflict between U.S. and foreign law does not change the best construction of an important domestic law enforcement and counterterrorism tool enacted more than 30 years ago." *Id.* at 52.

Second, the possibility of future legislation revising the Stored Communications Act likewise provides no basis to affirm the decision below. In opposing certiorari, Microsoft made much of pending legislation that would revise and update the Act. *See* Br. in Opp'n to Cert. 14-26; Supp. Br. in Opp'n to Cert. 1-3. Judge Lynch, too, called for legislative reform in the face of the absurd results created by the panel's decision. App. 68a-72a (Lynch, J., concurring); *see also In re Search Warrant*, 232 F. Supp. 3d at 723-25 (explaining why the Second Circuit's interpretation leads to absurd results). But the decision below is creating serious problems for law enforcement right now. The Court must decide this case under the legal framework currently in place, regardless of what Congress may do in the future.

Moreover, the Congress that enacted the Act was plainly concerned with maintaining a reasonable balance between the needs of law enforcement, service providers, and their customers, in the face of inevitable technological change. *See, e.g.*, 18 U.S.C. § 2703; 132 Cong. Rec. S7993 (daily ed. June 19, 1986) (statement of Sen. Leahy, co-sponsor of Senate bill) (explaining that the SCA was "designed to protect legitimate law enforcement needs while minimizing intrusions on the privacy of system users as well as the business needs of electronic communications system providers"); *Elec. Commc'n Privacy: Hearing on S. 1667 Before the Subcomm. on Patents, Copyrights, and Trademarks of the S. Comm. on the Judiciary*, 99th Cong. 39 (1985) (statement of Rep. Kastenmeier, lead sponsor of House

bill) ("We have attempted in [the Act] to describe the protection in more generic terms and not in technological terms, as far as possible, this for the purpose of making the law endure the test of time and presumably comprehend new technologies as they evolve.").[18] It is impossible to imagine that Congress intended to allow private business decisions to entirely control whether law enforcement can access key evidence in important, local, criminal investigations.

CONCLUSION

The decision below should be reversed.

December 13, 2017

Respectfully submitted,

THOMAS J. DONOVAN
Attorney General of the
State of Vermont
BENJAMIN D. BATTLES*
Solicitor General
ELEANOR L.P. SPOTTSWOOD
EVAN P. MEENAN
Assistant Attorneys General
109 State Street
Montpelier, VT 05609
(802) 828-5500
benjamin.battles@vermont.gov

Counsel of Record

[18] *Available at* https://www.justice.gov/sites/default/files/jmd/legacy/2014/07/19/hear-j-99-72-1985.pdf.

STEVE MARSHALL
Attorney General
STATE OF ALABAMA
501 Washington Avenue
Montgomery, AL 36130

LESLIE RUTLEDGE
Attorney General
STATE OF ARKANSAS
323 Center Street
Little Rock, AR 72201

CYNTHIA H. COFFMAN
Attorney General
STATE OF COLORADO
1300 Broadway
Denver, CO 80203

KEVIN T. KANE
Chief State's Attorney
STATE OF CONNECTICUT
300 Corporate Place
Rocky Hill, CT 06067

MATTHEW P. DENN
Attorney General
STATE OF DELAWARE
820 N. French Street
Wilmington, DE 19801

PAMELA JO BONDI
Attorney General
STATE OF FLORIDA
PL-01, The Capitol
Tallahassee, FL 32399

LISA MADIGAN
Attorney General
STATE OF ILLINOIS
100 W. Randolph St.
Chicago, IL 60601

CURTIS T. HILL, JR.
Attorney General
STATE OF INDIANA
200 W. Washington
Street
Indianapolis, IN 46204

THOMAS J. MILLER
Attorney General
STATE OF IOWA
1305 E. Walnut Street
Des Moines, IA 50319

DEREK SCHMIDT
Attorney General
STATE OF KANSAS
120 SW 10th Avenue
Topeka, KS 66612

ANDY BESHEAR
Attorney General
COMMONWEALTH
OF KENTUCKY
700 Capitol Avenue
Frankfort, KY 40601

JEFF LANDRY
Attorney General
STATE OF LOUISIANA
1885 N. Third Street
Baton Rouge, LA 70802

JANET T. MILLS
Attorney General
STATE OF MAINE
6 State House Station
Augusta, ME 04333

BRIAN E. FROSH
Attorney General
STATE OF MARYLAND
200 Saint Paul Place
Baltimore, MD 21202

MAURA HEALEY
Attorney General
COMMONWEALTH
OF MASSACHUSETTS
One Ashburton Place
Boston, MA 02108

BILL SCHUETTE
Attorney General
STATE OF MICHIGAN
P.O. Box 30212
Lansing, MI 48909

LORI SWANSON
Attorney General
STATE OF MINNESOTA
102 State Capitol
St. Paul, MN 55155

JIM HOOD
Attorney General
STATE OF MISSISSIPPI
P.O. Box 220
Jackson, MS 39205

TIMOTHY C. FOX
Attorney General
STATE OF MONTANA
P.O. Box 201401
Helena, MT 59620

DOUG PETERSON
Attorney General
STATE OF NEBRASKA
2115 State Capitol
Lincoln, NE 68509

ADAM PAUL LAXALT
Attorney General
STATE OF NEVADA
100 N. Carson Street
Carson City, NV 89701

CHRISTOPHER S. PORRINO
Attorney General
STATE OF NEW JERSEY
25 Market Street
Trenton, NJ 08625

HECTOR H. BALDERAS
Attorney General
STATE OF NEW MEXICO
408 Galisteo Street
Santa Fe, NM 87501

ERIC T. SCHNEIDERMAN
Attorney General
STATE OF NEW YORK
120 Broadway
New York, NY 10271

JOSH STEIN
Attorney General
STATE OF NORTH CAROLINA
9001 Mail Service Center
Raleigh, NC 27699

MICHAEL DEWINE
Attorney General
STATE OF OHIO
30 E. Broad Street
Columbus, OH 43215

MIKE HUNTER
Attorney General
STATE OF OKLAHOMA
313 NE 21st Street
Oklahoma City, OK 73105

ELLEN F. ROSENBLUM
Attorney General
STATE OF OREGON
1162 Court Street NE
Salem, OR 97301

JOSH SHAPIRO
Attorney General
COMMONWEALTH
OF PENNSYLVANIA
Strawberry Square
Harrisburg, PA 17120

PETER F. KILMARTIN
Attorney General
STATE OF RHODE ISLAND
150 S. Main Street
Providence, RI 02903

ALAN WILSON
Attorney General
STATE OF SOUTH CAROLINA
P.O. Box 11549
Columbia, SC 29211

KEN PAXTON
Attorney General
STATE OF TEXAS
P.O. Box 12548
Austin, TX 78711

MARK R. HERRING
Attorney General
COMMONWEALTH
OF VIRGINIA
202 N. Ninth Street
Richmond, VA 23219

PETER K. MICHAEL
Attorney General
STATE OF WYOMING
2320 Capitol Avenue
Cheyenne, WY 82002

WANDA VASQUEZ-GARCED
Attorney General
COMMONWEALTH
OF PUERTO RICO
P.O. Box 9020192
San Juan, PR 00902